Bounding the rank and determining the torsion of elliptic curves

Kaloyan Slavov

Final project for Math 129
Spring 2005

Abstract

We present a proof of the weak Mordell–Weil theorem that will enable us to explicitly bound the rank of certain classes of elliptic curves. We also discuss the Lutz–Nagel algorithm for determining the torsion subgroup. Finally, we determine the torsion subgroup of two special classes of elliptic curves. We follow [4] and [6].

1 Introduction.

That the group $E(\mathbb{Q})$ of rational point on an elliptic curve is finitely generated was conjectured by Poincarè in 1901 and proved by Mordell in 1922. Previous approaches to Diophantine equations were regarded by Poincarè, Hilbert, and others, as based on tricks rather than as a systematic theory ([5]).

In Section 1., we present a proof of the weak Mordell–Weil theorem, that the group $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, by exhibiting an explicit injective homomorphism $E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$ (in the case when there are four points of order dividing two) whose image is finite. To prove injectivity, we will need a characterization of the group $2E(\mathbb{Q})$, which will be the first theorem in the section. To prove finiteness of the image, we will use

divisibility properties in $\mathbb{Z}$ in the case when $E(\mathbb{Q})$ has four elements of order dividing 2. In the general case, we will replace $\mathbb{Z}$ by a suitable ring R that is a principal ideal domain and whose group of units is finitely generated.

Then the proof of the Mordell–Weil theorem can be finished easily by using "height" functions. This method is called "descent" because it generalizes Fermat's method of proving that the equation $x^4 + y^4 = z^2$ has no nontrivial solutions (which involves considering a solution and then obtaining a "smaller" one). In fact, Fermat's construction of a "smaller" solution is analogous to the construction of a point on the elliptic curve that is "simpler" arithmetically in the sense that it has a smaller height (for a more detailed discussion of the descent method, see [4], [6], [3], [5]).

In Section 2, we discuss the problem of determining the rank of an elliptic curve. We apply the previous injective homomorphism to find a bound on the rank in general. Then we examine more carefully the image of the homomorphism from before to further refine the rank. Yet more careful analysis of the possible image (using the theory of quadratic residues) will enable us to show that each curve in a certain class has rank 0, and to refine the bounds on the curves from another class. In general, the problem of computing the rank of an elliptic curve is extremely hard. For example, it is not known whether there are elliptic curves of arbitrarily large rank (the "folklore conjecture"). A curve of rank at least 24 was found in 2000 ([7]). John Cremona's program "mwrank" computes the ranks of elliptic curves (using the descent method), but no algorithm is known for computing the rank that can be proved to always terminate, for any elliptic curve E.

In Section 3., we first discuss the Lutz–Nagel theorem, which provides us with a simple algorithm for computing the torsion subgroup. Then, assuming the fact that the torsion subgroup injects into the group of points on E_p for p a prime of good reduction (this fact is also used in the Doud's algorithm which computes the torsion subgroup much more efficiently), we apply Dirichlet's theorem for the primes in an arithmetic progression to compute the torsion subgroups for two general classes of curves. Finally, in Section 4., we use the results obtained before to study the classical problem of congruent numbers.

2 Proof of the weak Mordell-Weil theorem.

Theorem 1. *Let*

$$E: \ y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

be an elliptic curve over a field K of characteristic 0, with $\alpha, \beta, \gamma \in K$. Then a point $(x_2, y_2) \in E(K)$ belongs to $2E(K)$ if and only if

$$x_2 - \alpha, x_2 - \beta, x_2 - \gamma$$

are squares in K.

Proof. First, assume that $(x_2, y_2) = 2(x_1, y_1)$ for some $(x_1, y_1) \in E(K)$ (then $x_1 \notin \{\alpha, \beta, \gamma\}$ because $(x_2, y_2) \neq \mathcal{O}$). If $y = mx + b$ is the line tangent to E at x_1, then by the definition of addition in $E(K)$, we have

$$(x - \alpha)(x - \beta)(x - \gamma) - (mx + b)^2 = (x - x_1)^2(x - x_2).$$

Set $x = \alpha$ to conclude that $x_2 - \alpha = (\frac{m\alpha+b}{\alpha-x_1})^2$ is a square in K, and similarly for $x_2 - \beta$ and $x_2 - \gamma$.

For the other direction, assume without loss of generality that $x_2 = 0$ (we can make a change of variable $x \mapsto x - x_2$, which just translates the curve), and $-\alpha = a^2$, $-\beta = b^2$, $-\gamma = c^2$ (with $a, b, c \in K$). We can adjust the signs of a, b, c so that $abc = -y_2$. We have to produce (x_1, y_1) so that if $y = mx - y_2$ is the tangent line to the curve at x_1, then $(x-\alpha)(x-\beta)(x-\gamma)-(mx-y_2)^2 = (x - x_1)^2 x$. We claim that it suffices to find $m \in K$ such that

$$\frac{(x - \alpha)(x - \beta)(x - \gamma) - (mx - y_2)^2}{x} = (x - x_1)^2 \tag{1}$$

for some x_1. Indeed, in such a case, $(x_1, mx_1 - y_2) \in E(K)$; since x_1 is a double root of the left hand side of (1), the tangent line to E at (x_1, y_1) (where $y_1 = mx_1 - y_2$) indeed has the form $y = mx + b$, and necessarily $b = -y_2$ because it has to pass through $(0, -y_1)$. Then, by definition, $2(x_1, y_1) = (0, -(m.0 - y_2)) = (0, y_2)$.

Write $(x - \alpha)(x - \beta)(x - \gamma) = x^3 + rx^2 + sx + y_2^2$; then (1) will follow if the equation $x^2 + (r - m^2)x + (s + 2my_2)$ has a double root, or, equivalently, discriminant 0. However, one can check that $(m^2 - r)^2 = 4(s + 2my_2)$ is equivalent to $(m^2 - r - 2\alpha)^2 = 4(am - bc)^2$. So, it suffices to find a solution of $m^2 - \alpha + \beta + \gamma = 2(am - bc)$, and the last equation is $(m - a)^2 = (b - c)^2$, which indeed has a solution for m in K. □

Proposition 2. *Let*

$$E : \ y^2 = (x - \alpha)(x - \beta)(x - \gamma)$$

be an elliptic curve over $\mathbb{Q}$ *with* $\alpha, \beta, \gamma \in \mathbb{Z}$. *Then the map*

$$\varphi: \ E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 \qquad \textit{given by}$$

$$\varphi(P) = \begin{cases} 1, & \textit{if} \quad P = \mathcal{O} \\ \overline{(\alpha-\beta)(\alpha-\gamma)}, & \textit{if} \quad P = (\alpha, 0) \\ \overline{x-\alpha}, & \textit{if} \quad P = (x,y), \ x \neq \alpha, \ P \neq \mathcal{O} \end{cases}$$

is a group homomorphism.

Proof. Notice that given a point $P \in E(\mathbb{Q})$, the first coordinate of $-P$ is the same as the one of P, hence $\varphi(-P) = \varphi(P)$. Also, $\varphi(P)^2 = 1$, hence $\varphi(P)^{-1} = \varphi(P)$. Thus, to check that $P_1 + P_2 = P_3$ implies $\varphi(P_1)\varphi(P_2) = \varphi(P_3)$ is to check that $P_1 + P_2 + P_3 = \mathcal{O}$ implies $\varphi(P_1)\varphi(P_2)\varphi(P_3) = (\mathbb{Q}^*)^2$. So, let $P_1 + P_2 + P_3 = \mathcal{O}$.

If $P_1 = \mathcal{O}$, then $\varphi(P_2) = \varphi(P_3)$ and the conclusion follows. Assume $P_1, P_2, P_3 \neq \mathcal{O}$, $P_i = (x_i, y_i)$. Then P_1, P_2, P_3 lie on a line $y = mx + b$ (where $m, b \in \mathbb{Q}$) and

$$(x-\alpha)(x-\beta)(x-\gamma) - (mx+b)^2 = (x-x_1)(x-x_2)(x-x_3). \qquad (2)$$

If $x_i \neq \alpha$ for any i, then we set $x = \alpha$ to deduce $(x_1-\alpha)(x_2-\alpha)(x_3-\alpha) = (m\alpha+b)^2$, hence $\varphi(P_1)\varphi(P_2)\varphi(P_3) = (m\alpha+b)^2(\mathbb{Q}^*)^2 = (\mathbb{Q}^*)^2$, as desired. If $(x_1, y_1) = (\alpha, 0)$, then $x_2, x_3 \neq \alpha$ (since we assume $P_2, P_3 \neq \mathcal{O}$). Then (2) implies that $x - \alpha$ divides the polynomial $(mx+b)^2$, so $mx + b = m(x-\alpha)$. Substituting it in (2) yields $(x-\beta)(x-\gamma) - m^2(x-\alpha) = (x-x_2)(x-x_3)$ after cancellation by $(x-\alpha)$. Set $x = \alpha$ to conclude $(\alpha-\beta)(\alpha-\gamma) = (\alpha-x_2)(\alpha-x_3)$. In other words, $\varphi(P_1) = \varphi(P_2)\varphi(P_3)$, hence $\varphi(P_1)\varphi(P_2)\varphi(P_3) = \varphi(P_1)^2 = (\mathbb{Q}^*)^2$, as desired. □

Therefore, $\varphi(2P) = \varphi(P)^2 = (\mathbb{Q}^*)^2$, hence $\varphi = \varphi_\alpha$ induces a group homomorphism

$$\varphi_\alpha: \ E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2.$$

Similarly, we have a group homomorphism

$$\varphi_\beta: \ E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 \qquad \text{given by}$$

$$\varphi_\beta(P) = \begin{cases} 1, & \text{if} \quad P = \mathcal{O} \\ \overline{(\beta-\alpha)(\beta-\gamma)}, & \text{if} \quad P = (\beta, 0) \\ \overline{x-\beta}, & \text{if} \quad P = (x,y), \ x \neq \beta, \ P \neq \mathcal{O}. \end{cases}$$

Proposition 3. *The map*

$$\varphi_\alpha \times \varphi_\beta : \ E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \tag{3}$$

is injective.

Proof. Let $\varphi_\alpha(P) = (\mathbb{Q}^*)^2$, $\varphi_\beta(P) = (\mathbb{Q}^*)^2$, where $P = (x_2, y_2)$. If $x_2 \neq \alpha, x_2 \neq \beta$, then the condition is that $x_2 - \alpha$ and $x_2 - \beta$ are squares in $\mathbb{Q}$, hence $(x_2-\alpha)(x_2-\beta)(x_2-\gamma) = y_2^2$ implies that $x_2-\gamma$ is a square, too. Thus, Theorem 1 implies that $(x_2, y_2) \in 2E(\mathbb{Q})$. If $x_2 = \alpha$, then the definitions of φ_α and φ_β yield that $(\alpha-\beta)(\alpha-\gamma)$ and $(\alpha-\beta)$ are squares in $\mathbb{Q}$. But then $(\alpha-\gamma)$ is a square, and since so is $\alpha-\alpha = 0$. We have that the numbers $x_2-\alpha, x_2-\beta, x_2-\gamma$ are all squares, hence Theorem 1 again implies that $P \in 2E(\mathbb{Q})$. □

We write

$$\mathbb{Q}^*/(\mathbb{Q}^*)^2 = \{\epsilon 2^{a_1}3^{a_2}... \mid \epsilon \in \{\pm 1\},\ a_i \in \{0,1\}, \text{almost all } a_i = 0\} = \bigoplus_{\pm, p\text{–prime}} \mathbb{Z}/2\mathbb{Z}.$$

Proposition 4. *If E is as in Proposition 2 (i.e., $\alpha, \beta, \gamma \in \mathbb{Z}$), and*

$$d = (\alpha-\beta)^2(\beta-\gamma)^2(\gamma-\alpha)^2$$

is the discriminant of the cubic defining the elliptic curve, then the image of $\varphi_\alpha \times \varphi_\beta$ is contained in the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ that has zeroes in all coordinates except the ones corresponding to ± 1 and primes $p|d$.

Proof. For a prime p and $s \in \mathbb{Q}^*$, we say that $p^k||s$ is $s = p^k s'$, where p is coprime to both the numerator and denominator of s' when written in lowest terms. Let $p \nmid d$ (i.e., $p \nmid (\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)$) be a prime number, and let $(x, y) \in E(\mathbb{Q}) - \{\mathcal{O}\}$. If $x \in \{\alpha, \beta, \gamma\}$, then $\varphi_\alpha(x, y)$ and $\varphi_\beta(x, y)$ are products of $(\alpha-\beta)$, $(\beta-\gamma)$, and $(\gamma-\alpha)$, so neither of them is divisible by p. Assume from now on that $x \notin \{\alpha, \beta, \gamma\}$. If a, b, c are the integers satisfying $p^a||(x-\alpha)$, $p^b||(x-\beta)$, $p^c||(x-\gamma)$, then the fact that $(x-\alpha)(x-\beta)(x-\gamma) = y^2 \in \mathbb{Q}^*$ implies that

$$a + b + c \equiv 0 \pmod 2.$$

Assume first that $a = -k < 0$. Then $x \neq 0$ (since $\alpha \in \mathbb{Z}$), so we can write $x = \frac{x'}{x''}$ with $\gcd(x', x'') = 1$. Since $p^{-k}||\frac{x'-\alpha x''}{x''}$, it follows first that $p^k|x''$, but then $p \nmid x'$, hence $p^k||x''$. Next, it follows that $p^{-k}||(x-\beta)$ and

$p^{-k}||(x-\gamma)$, so $a=b=c$, hence each of a,b,c is even. But $(\varphi_\alpha \times \varphi_\beta)(x,y) = \overline{(x-\alpha)(x-\beta)}$, and since $a+b$ is even, the coordinate corresponding to p in $\mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$ is indeed $(0,0)$.

Now assume at least one of a,b,c, say a, is positive. Then $(x-\alpha) = p^a \frac{a'}{a''}$, and since $p \nmid (\alpha-\beta)$, we have that $x-\beta = (x-\alpha)+(\alpha-\beta) = \frac{p^a a' + a''(\alpha-\beta)}{a''}$ does not have p in its numerator, so $b=0$, and analogously $c=0$. Thus, a is even, so again the power of p dividing each of $x-\alpha$ and $x-\beta$ is even, hence $(x-\alpha, x-\beta)$ has $(0,0)$ in its $p-$th coordinate in $\mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$. $\square$

This finishes the proof in the case where $\alpha,\beta,\gamma \in \mathbb{Q}$ (since in this case, they have to be integers). In the general case, let $K = \mathbb{Q}(\alpha,\beta,\gamma)$. We proved in class that it suffices to show that $E(K)/2E(K)$ is finite. Let $\mathcal{R}$, $\mathcal{O}_K \subset \mathcal{R} \subset K$ be a ring which is a principal ideal domain, and whose group U of units is finitely generated (we established its existence in class). The field of fractions of $\mathcal{R}$ is still K, so $\mathcal{R}$ will play the role $\mathbb{Z}$ has in the particular case of the theorem. Since U is a finitely generated abelian group, U/U^2 is finite, and we have as before that

$$K^*/(K^*)^2 \simeq (U/U^2) \times \bigoplus_{P\text{–prime in } \mathcal{R}} \mathbb{Z}/2\mathbb{Z}.$$

The proof we have given before carries over, and the existence of an injective homomorphism

$$E(K)/2E(K) \longrightarrow \left((U/U^2) \times \bigoplus_{P\text{–prime of } \mathcal{R}, P|D} \mathbb{Z}/2\mathbb{Z} \right) \times \left((U/U^2) \times \bigoplus_{P\text{–prime of } \mathcal{R}, P|D} \mathbb{Z}/2\mathbb{Z} \right).$$

(where again $D \in \mathbb{Z}$ is the discriminant of the cubic $(x-\alpha)(x-\beta)(x-\gamma)$ and divisibility is in $\mathcal{R}$) finishes the proof of the weak Morderl–Weil theorem.

Using "height" functions, one can deduce the Mordell-Weil theorem:

Theorem 5. *If $E: y^2 = x^3 + ax + b$ is an elliptic curve over $\mathbb{Q}$, then the group $E(\mathbb{Q})$ is finitely generated, hence*

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{tor}.$$

3 Determining the rank.

Lemma 6. *Suppose* $|E(\mathbb{Q})/2E(\mathbb{Q})| \leq 2^l$, *where* $E : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ *is an elliptic curve over* $\mathbb{Q}$ *with* $\alpha, \beta, \gamma \in \mathbb{Z}$. *Then the rank* r *of* E *satisfies* $r \leq l-2$.

Proof. The points of order dividing 2 on E (i.e., $\mathcal{O}, (\alpha, 0), (\beta, 0), (\gamma, 0)$) form a subgroup $\mathbb{Z}/2 \times \mathbb{Z}/2 \subset E(\mathbb{Q})$; if s is even, then $\mathbb{Z}/s\mathbb{Z}$ has an element of order 2. This implies that $E(\mathbb{Q}) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2 \times M \times \mathbb{Z}^r$, where M is a finite torsion group of odd order. Therefore, $|E(\mathbb{Q})/2E(\mathbb{Q})| = 2^{2+r}$, hence $r+2 \leq l$, as desired. □

Given an elliptic curve $E : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ with $\alpha, \beta, \gamma \in \mathbb{Z}$, we say that a prime p is *fairly bad* if p divides only one of $\alpha-\beta, \beta-\gamma, \gamma-\alpha$, and *very bad* if p divides all three of them (of course, if it divides two of them, then it divides the third one, as well).

Proposition 7. *If* n_1 *denotes the number of fairly bad primes, and* n_2 *denotes the number of very bad primes, then there is an injective map*

$$E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathbb{Z}/2 \times \underbrace{\mathbb{Z}/2 \times \cdots \times \mathbb{Z}/2}_{n_1} \times \prod_{n_2 \text{ copies}} (\mathbb{Z}/2 \times \mathbb{Z}/2),$$

hence the rank r *of* E *satisfies*

$$r \leq n_1 + 2n_2 - 1.$$

Proof. We can assume without loss of generality that $\alpha < \beta < \gamma$, for if this is not the ordering of the three numbers, we can consider the product of two other homomorphisms among $\varphi_\alpha, \varphi_\beta$, and φ_γ, instead of $\varphi_\alpha \times \varphi_\beta$. If $P = (x, y) \in E(\mathbb{Q}) - \{\mathcal{O}\}$, then $x-\alpha > x-\beta > x-\gamma$, and since $(x-\alpha)(x-\beta)(x-\gamma) = y^2 \geq 0$, necessarily $x-\alpha \geq 0$. If $x \notin \{\alpha, \beta, \gamma\}$, then φ_α maps (x, y) to $(x-\alpha)$, which is positive. If $x = \alpha$, then $\varphi_\alpha(x, y) = (\alpha-\beta)(\alpha-\gamma) > 0$ by the ordering. Similarly, if $x = \beta$ or $x = \gamma$, then $x-\alpha > 0$. Thus, the image of $E(\mathbb{Q})/2E(\mathbb{Q})$ under $\varphi_\alpha \times \varphi_\beta$ is contained in the subgroup of elements whose ± 1 coordinates correspond to $0 \times \mathbb{Z}/2$. So, the first factor $\mathbb{Z}/2 \times \mathbb{Z}/2$ corresponding to the ± 1 coordinate in (3) can be replaced by a single $\mathbb{Z}/2$.

Let p be a fairly bad prime. We will show that, similarly, the factor $\mathbb{Z}/2 \times \mathbb{Z}/2$ corrsponding to the prime p in (3) can be replaced by a single $\mathbb{Z}/2$.

In other words, there is a two–element subgroup $M \subset \mathbb{Z}/2 \times \mathbb{Z}/2$ (depending on p) such that the $p-$th coordinate of $\varphi_\alpha \times \varphi_\beta(P)$ is contained in M for any $P \in E(\mathbb{Q})$.

Assume that $p|(\alpha - \beta)$, hence $p \nmid (\beta - \gamma)$ and $p \nmid (\gamma - \alpha)$. We will show that we can take $M =< 1, 1 >= \text{diag}(\mathbb{Z}/2 \times \mathbb{Z}/2)$. If $p|(\beta - \gamma)$, a similar argument will show that we can take $M = 0 \times \mathbb{Z}/2$, and if $p|(\gamma - \alpha)$, we can take $M = \mathbb{Z}/2 \times 0$.

Consider a point $P = (x, y) \in E(\mathbb{Q})$. If $x = \alpha$, then $\varphi_\alpha(P) = \overline{(\alpha - \beta)(\alpha - \gamma)}$, and $\varphi_\beta(P) = \overline{(\alpha - \beta)}$, and these two rationals have the same power of p in their factorization, since $p \nmid (\alpha - \gamma)$. Similarly, if $x = \beta$, then $\varphi_\alpha(P) = \overline{\beta - \alpha}$ and $\varphi_\beta(P) = \overline{(\beta - \alpha)(\beta - \gamma)}$, which again have the same power of p in their factorizations. Finally, $x = \gamma$ yields $\varphi_\alpha(P) = \overline{(\gamma - \alpha)}$ and $\varphi_\beta(P) = \overline{(\gamma - \beta)}$, and these two are both not divisible by p.

Assume $x \notin \{\alpha, \beta, \gamma\}$. We can define integers a, b, c as above by $p^a||(x-\alpha)$, $p^b||(x - \beta)$, $p^c||(x - \gamma)$. We know that $a + b + c \equiv 0 \pmod 2$, and we have to deduce $a \equiv b \pmod 2$ in order to conclude that indeed $\varphi_\alpha \times \varphi_\beta(P) \in \text{diag}(\mathbb{Z}/2 \times \mathbb{Z}/2)$. Here we will use the condition that p is fairly bad. If one of a, b, c is negative, we saw that $a = b = c$, so assume all of them are nonnegative. Assume first $a > 0$. Then $x - \alpha = p^a \frac{a'}{a''}$ with $\gcd(p, a') = \gcd(p, a'') = 1$. If $c > 0$, it follows that $\alpha - \gamma = (\alpha - x) + (x - \gamma)$ is divisible by p, which is a contradiction. So, $c = 0$, hence indeed $a + b \equiv 0 \pmod 2$. Similarly, $b > 0$ implies $c = 0$. If $c > 0$, then the same reasoning yields $a = 0$ and $b = 0$, so again $a \equiv b \pmod 2$. Finally, if $a = b = c = 0$, there is nothing to prove. □

Proposition 8. *Consider the elliptic curve*

$$E : y^2 = x^3 - p^2x^2,$$

where $p \neq 2$ is a prime number. The rank r of E satisfies

- $r \leq 2$ *if* $p \equiv 1 \pmod 8$
- $r = 0$ *if* $p \equiv 3 \pmod 8$
- $r \leq 1$ *if* $p \equiv 5, 7 \pmod 8$.

Proof. Set $\alpha = -p, \beta = 0, \gamma = p$. Then 2 is a fairly bad prime, while p is a very bad prime, hence we know a priori only that $r \leq 2$ regardless of p.

We now sharpen the estimation by looking more closely at the images of $\varphi_\alpha, \varphi_\beta, \varphi_\gamma$.

Consider a point $P = (x, y) \in E(\mathbb{Q})$ with $x \notin \{\alpha, \beta, \gamma\}$. Then $\varphi_\alpha(P) = x + p, \varphi_\beta(P) = x, \varphi_\gamma(p) = x - p$. Since $(x + p)x(x - p) = y^2$, we have either $x + p > 0$ and $x < 0, x - p < 0$, or $x + p > 0, x < 0, x - p > 0$. Since $2|(\gamma - \alpha)$, the proof of the previous Proposition implies that $\varphi_\beta(P)$ has 0 in its $2-$coordinate, and since the product of the three numbers $x+p, x, x-p$ is a square, the only possibilities for the $2-$coordinate of $(\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma)(P)$ are $(0, 0, 0)$ and $(1, 0, 1)$. Similarly, if the power of p dividing one of $x+p, x, x-p$ is odd, then the power of p in precisely another one of these three numbers is odd. Thus, the possible triples for the $p-$coordinate of $(\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma)(P)$ are $(0, 0, 0), (0, 1, 1), (1, 0, 1), (1, 1, 0)$. We compute directly that

$$\begin{aligned}(\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma)(\alpha, 0) &= (2p^2, -p, -2p),\\ (\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma)(\beta, 0) &= (p, -p^2, -p),\\ (\varphi_\alpha \times \varphi_\beta \times \varphi_\gamma)(\gamma, 0) &= (2p, p, 2p^2).\end{aligned}$$

So, the $p-$coordinates of the images of $(\alpha, 0), (\beta, 0), (\gamma, 0)$ under $\varphi = \varphi_\alpha \times \varphi_\beta \times \varphi_\beta$ are respectively $(0, 1, 1), (1, 0, 1), (1, 1, 0)$, hence all three nontrivial triples for the $p-$coordinate occur. The key idea is based on this observation. For any $P = (x, y) \in E(\mathbb{Q})$, there is $R_P \in \{\mathcal{O}, (\alpha, 0), (\beta, 0), (\gamma, 0)\}$ such that $\varphi(P)$ and $\varphi(R_P)$ have the same $p-$ coordinate, so the $p-$th coordinate of $\varphi(P + R_P)$ will be the triple $(0, 0, 0)$. Consider the set–theoretic map

$$\begin{gathered}\varphi' : E(\mathbb{Q})/2E(\mathbb{Q}) \longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \qquad \text{given by}\\ P = (x, y) \longmapsto (\varphi_\alpha(P + R_P), \varphi_\beta(P + R_P), \varphi_\gamma(P + R_P)).\end{gathered}$$

If $\varphi'(P) = \varphi'(P')$, then $P - P' \in \{\mathcal{O}, (\alpha, 0), (\beta, 0), (\gamma, 0)\}$, so there are four possible preimages of each element in the target. In particular, if $|\mathrm{im}(\varphi')| \leq 2^l$, then $|E(\mathbb{Q})/2E(\mathbb{Q})| \leq 4.2^l = 2^{l+2}$, so $r \leq l$.

Since the $p-$coordinate of φ' is always trivial, and the possibilities for the $\pm-$coordinate are $(+, +, +), (+, -, -)$ while the possibilities for the $2-$coordinate are $(0, 0, 0), (1, 0, 1)$, there are at most four cases, but we can limit them further using the theory of quadratic residues. One can easily show that if there is $x \in \mathbb{Q}$ with $x + p = a_1^2, x = -a_2^2, x - p = -a_3^2$ $(a_1, a_2, a_3 \in \mathbb{Q})$ then $p \equiv 1, 5 \pmod 8$. Also, if the situation $x + p = 2a_1^2, x = a_2^2, x - p = 2a_3^2$, occurs, then $p \equiv 1, 7 \pmod 8$, and if $x + p = 2a_1^2, x = -a_2^2, x - p = -2a_3^2$, then $p \equiv 1 \pmod 8$.

In conclusion, if $p \equiv 3 \pmod 8$, then only one case can occur, so $|\mathrm{im}(\varphi')| \leq 1 = 2^0$, hence $r = 0$. If $p \equiv 5 \pmod 8$, then the only possibilities for the $\pm$ and $2-$coordinates are $(+,+,+),(0,0,0)$ and $(+,-,-),(0,0,0)$, hence at most $2 = 2^1$ possibilities, hence $r \leq 1$. If $p \equiv 7 \pmod 8$, the only possibilities are $(+,+,+),(0,0,0)$ and $(+,+,+),(0,1,0)$, hence again two possibilities and so $r \leq 1$. □

4 Determining the torsion subgroup.

4.1 The Lutz-Nagel algorithm.

Theorem 9. *If $E : y^2 = x^3 + ax^2 + bx + c$ is an elliptic curve over $\mathbb{Q}$ with $a, b, c \in \mathbb{Z}$, and if D is the discriminant of $x^3 + ax^2 + bx + c$, then any point $(x, y) \in E(\mathbb{Q})$ of finite order has integer coordinates, and $y = 0$ or $y|D$.*

Since there are finitely many y_0 with $y_0 = 0$ or $y_0|D$, and for each y_0 there are finitely many rational solutions of $y_0^2 = x^3 + ax^2 + bx + c$, which we can determine explicitly, we can compute a finite set S of rational points that contains all possible torsion points in $E(\mathbb{Q})$. For each $P \in S$, we may start adding P to itself in order to determine if P is a torsion point, and if so, to determine its order. Of course, if we do not get that $(\#S)P = \mathcal{O}$, then P is not a torsion point. Thus, we have an algorithm whose output is the number of torsion points of any given order, which determines the torsion subgroup $E(\mathbb{Q})_{\mathrm{tor}}$ uniquely. Of course, in practice we may simplify the computations assuming, for instance, Mazur's theorem (according to which the torsion subgroup is either $\mathbb{Z}/m\mathbb{Z}$ for $1 \leq m \leq 10$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ for $1 \leq m \leq 4$). Namely, we have to examine only $m \leq 12$ such that $mP = \mathcal{O}$ to determine the order of P.

More concretely, Darrin Doud's algorithm ([2]) is much faster than the Lutz-Nagel algorithm. First, it uses that for a prime p of good reduction, there is an injection $E(\mathbb{Q})_{\mathrm{tor}} \hookrightarrow E_p(\mathbb{Z}/p\mathbb{Z})$. Thus, by computing the order of $E_p(\mathbb{Z}/p\mathbb{Z})$ for several small values of p, we may obtain a bound b such that $|E_p(\mathbb{Z}/p\mathbb{Z})|$ divides b. Then the analysis splits into two cases depending on whether 4 divides b or not (for if $4 \nmid b$, then the torsion subgroup must be cyclic, by Mazur's theorem) and involves looking at suitable points on $E(\mathbb{C})$ and checking whether they are rational.

Proof. The case $y = 0$ is clear, so we may consider only points with $y \neq 0$.

Fix a prime p. Consider a point $(x, y) \in E(\mathbb{Q})$ with $\mathrm{ord}_p(y) = -\sigma < 0$, i.e., $y = \frac{u}{wp^\sigma}$. If $x = \frac{m}{np^\mu}$, we get that

$$\frac{u^2}{w^2 p^{2\sigma}} = \frac{m^3 + am^2 np^\mu + bmn^2 p^{2\mu} + cn^3 p^{3\mu}}{n^3 p^{3\mu}}.$$

If $\mu \leq 0$, the order of p on the RHS is greater than or equal to zero, but it has to equal -2σ, so $\mu > 0$ and thus $-2\sigma = -3\mu$. Similarly, $\mu > 0$ implies $\sigma > 0$ and again $2\sigma = 3\mu$. In this case, $\mu = 2\lambda$ and $\sigma = 3\lambda$, so (x, y) belongs to the set

$$C(p^\lambda) = \{(x, y) \in E(\mathbb{Q}) \mid \mathrm{ord}_p(x) \leq -2\lambda,\ \mathrm{ord}_p(y) \leq -3\lambda\} \cup \{\mathcal{O}\}.$$

Notice that

$$E(\mathbb{Q}) \supset C(p^1) \supset C(p^2) \supset \cdots \supset C(p^\lambda) \supset \ldots$$

and that $(x, y) \in C(p^\lambda)$ implies $y \neq 0$ (since the coefficients of E are integers). It suffices to show that $C(p)$ contains no nontrivial points of finite order. Indeed, since p was arbitrary, it will follow that the denominator of any rational point of finite order is not divisible by any primes, so the point must have integer coordinates.

Consider the ring $R = \{x \in \mathbb{Q} \mid \mathrm{ord}_p(x) \geq 0\}$ obtained by turning every prime $q \neq p$ into a unit, in which p is the only prime. For $P = (x, y) \in E(\mathbb{Q})$ with $y \neq 0$, define $t(P) = \frac{x}{y}$. Set $t(\mathcal{O}) = 0$. If $x = \frac{m}{np^{2\lambda}}$ and $y = \frac{u}{wp^{3\lambda}}$, then $\frac{x}{y} = \frac{xw}{nu} p^\lambda$, so $t(x, y) \in p^\lambda R$. By the previous remarks, the converse is also true, so $(x, y) \in C(p^\lambda)$ if and only if $t(x, y) \in p^l R$. Thus the map t keeps track of the fact that the power of p in the denominators of x and y has the form 2λ and 3λ respectively. It can be shown by tedious computation involving the explicit formulas for the sum of two points on an elliptic curve and by using the change of variables $x' = \frac{x}{y}, y' = \frac{1}{y}$ that each $C(p^\lambda)$ is a subgroup of $E(\mathbb{Q})$ and for any $P_1, P_2 \in C(p^\lambda)$,

$$t(P_1) + t(P_2) \equiv t(P_1 + P_2) \pmod{p^{3\lambda} R}. \tag{4}$$

Assume for the sake of contradiction that $P = (x, y) \in C(p) - \{\mathcal{O}\}$ has finite order $m > 1$. Then $y \neq 0$ and there is a power of p which does not divide the denominator of y, so there is some λ with $P \notin C(p^{\lambda+1})$ but $P \in C(p^l)$.

If $p \nmid m$, since $C(p) \subset E(\mathbb{Q})$ is a subgroup, we have that $P, 2P, ..., mP \in C(P)$, so the congruence (4) yields

$$0 = t(\mathcal{O}) = t(mP) = t(\underbrace{P + \cdots + P}_{m}) \equiv mt(P) \pmod{p^{3\lambda}R},$$

hence $mt(P) \in p^{3\lambda}R$. Since m is prime to p, the definition of R implies that $t(P) \in p^{3\lambda}R$, hence $P \in C(p^{3\lambda})$. This contradicts the maximality of λ with $P \in C(p^l)$.

If $p|m$, write $m = pk$. Consider the point $Q = kP \in C(p)$. The order of Q in $E(\mathbb{Q})$ is p, and we can again find some largest λ with $Q \in C(p^\lambda)$ (of course, $\lambda > 0$). As in the previous case,

$$0 = t(\mathcal{O}) = t(pQ) \equiv pt(Q) \pmod{p^{3\lambda}R},$$

which shows that $t(Q) \in p^{3\lambda-1}R$. This contradicts the maximality of λ because $3\lambda - 1 > \lambda$, and finishes the proof of the first part.

To establish the divisibility statement, consider a point $P = (x, y) \in E(\mathbb{Q})$ of finite order with $y \neq 0$ (we know that $x, y \in \mathbb{Z}$). Then the order of $2P$ is finite, too, and $2P \neq \mathcal{O}$. Write $2P = (u, v)$ with $u, v \in \mathbb{Z}$. The formula for the $x-$coordinate of $2P$ implies that

$$u = \left(\frac{f'(x)}{2y}\right)^2 - a - 2x,$$

so $\left(\frac{f'(x)}{2y}\right)^2 \in \mathbb{Z}$, hence $\left(\frac{f'(x)}{2y}\right) \in \mathbb{Z}$. So, $y|f'(x)$. Of course, y also divides $f(x)$ because $y^2 = f(x)$. It is known[1] that $D \in \mathbb{Z}[t]f(t) + \mathbb{Z}[t]f'(t)$, so plugging $t = x$ shows that $D \in \mathbb{Z}f(x) + \mathbb{Z}f'(x)$. Therefore, $y|D$, as desired. □

4.2 The torsion subgroup for two classes of curves.

We will explicitly determine the torsion subgroup for two classes of curves by using the result that for a prime p not dividing the discriminant of the cubic $x^3 + ax^2 + bx + c$ defining an elliptic curve $E : y^2 = x^3 + ax^2 + bx + c$, there is an injection

$$r_p : E(\mathbb{Q})_{\text{tor}} \hookrightarrow E_p(\mathbb{Z}/p\mathbb{Z}).$$

[1]See [6], p. 48 for the explicit formula.

Proposition 10. *Consider the elliptic curve*

$$E : y^2 = x^3 + Ax,$$

where the integer A is fourth-power free. Then

$$E(\mathbb{Q})_{tor} = \begin{cases} \mathbb{Z}/2 \oplus \mathbb{Z}/2 & \text{if} \quad -A \quad \text{is a square,} \\ \mathbb{Z}/4 & \text{if} \quad A = 4, \\ \mathbb{Z}/2 & \text{otherwise.} \end{cases}$$

Proof. First we count $|E_p(\mathbb{Z}/p)|$ for $p \equiv 3 \pmod 4$. For each $x \in \mathbb{Z}/p$, we consider $x^3 + Ax \in \mathbb{Z}/p$, and notice that if it is a nonzero square in $\mathbb{Z}/p$, then it has two square roots, hence it yields two solutions, and if it is not a square, it yields no solutions. For $x \neq 0$, if $x^3 + Ax \neq 0$, then exactly one of $x^3 + Ax$ and $-(x^3 + Ax) = (-x)^3 + A(-x)$ is a square (by quadratic residues theory, -1 is not a square). If $x^3 + Ax = 0$, then each of x and $-x$ induces a single solution. Thus, a pair $\{x, -x\}$ induces two solutions of the equation. Therefore, counting the point at infinity, we obtain $2\frac{p-1}{2} + 1 + 1 = p + 1$ elements in $E_p(\mathbb{Z}/p)$.

We claim that $|E(\mathbb{Q})_{\text{tor}}|$ divides 4. Use Dirichlet's theorem to find a prime $p \equiv 3 \pmod 8$ that does not divide the discriminant of the curve. Since there is an inclusion $E(\mathbb{Q})_{\text{tor}} \hookrightarrow E_p(\mathbb{Z}/p)$, it follows that $|E(\mathbb{Q})_{\text{tor}}|$ divides $|E_p(\mathbb{Z}/p)| = p + 1 \equiv 4 \pmod 8$, hence $|E(\mathbb{Q})_{\text{tor}}|$ is not divisible by 8. Choose a prime of good reduction $p \equiv 7 \pmod{12}$ and notice that $|E(\mathbb{Q})_{\text{tor}}|$ divides $p + 1 \equiv 8 \pmod{12}$, hence is not divisible by 3. Finally, if $q > 3$ is any prime, and $p \equiv 3 \pmod{4q}$ is a prime of good reduction, then $p + 1 \equiv 4 \pmod{4q}$ is not divisible by q, hence neither is $|E(\mathbb{Q})_{\text{tor}}|$.

On the other hand, $(0, 0)$ is an element of order 2 in $E(\mathbb{Q})$. If $A = 4$, we have $(0, 0) = 2.(2, 4)$ because of the formula

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}$$

for the $x-$coordinate of the point $2P = 2(x, y)$ on an elliptic curve $y^2 = x^3 + Ax + B$ (here $B = 0$). So, the torsion subgroup is $\mathbb{Z}/4$ when $A = 4$. If $-A$ is a square, then $x^3 + Ax$ has three roots in $\mathbb{Q}$, hence $E(\mathbb{Q})$ has three elements of order 2, hence $E(\mathbb{Q})_{\text{tor}} = \mathbb{Z}/2 \oplus \mathbb{Z}/2$ in this case. Finally, if $-A$ is not a square, it suffices to show that $(0, 0) \notin 2E(\mathbb{Q})$ to conclude that

$E(\mathbb{Q})_{\text{tor}} = \mathbb{Z}/2$. Assume $(0,0) = 2(x,y)$; it follows that $x^4 - 2Ax^2 + A^2 = 0$, so $(x^2 - A)^2 = 0$, thus $x^2 = A$. But A is not divisible by the fourth power of a prime, so x is square-free. However, $y^2 = x^3 + Ax = x(x^2 + A) = x.2x^2 = 2x^3$, which implies that x is not divisible by an odd number, so $x = \pm 1, \pm 2$. Then we see that $x \neq \pm 1$, so $A = 4$, but we already dealt with this case. □

Proposition 11. *Consider the elliptic curve*

$$E : y^2 = x^3 + B,$$

where $B \in \mathbb{Z}$ is not divisible by a sixth power of a prime. Then

$$E(\mathbb{Q})_{tor} = \begin{cases} \mathbb{Z}/6, & \text{if } B = 1 \\ \mathbb{Z}/3, & \text{if } B = -2^4 3^3 \text{ or } B \neq 1 \text{ is a square} \\ \mathbb{Z}/2, & \text{if } B \neq 1 \text{ is a cube} \\ 0, & \text{otherwise.} \end{cases}$$

Proof. We first show that $|E_p(\mathbb{Z}/p)| = p + 1$ for $p \equiv 2 \pmod 3$. Since 3 does not divide $p - 1 = |(\mathbb{Z}/p)^*|$, there are no elements of order 3 in $(\mathbb{Z}/pZ)^*$, so the homomorphism $a \mapsto a^3$ is injective, hence bijective. Since 0 has a unique cube root in $\mathbb{Z}/p\mathbb{Z}$, this shows that any element in $\mathbb{Z}/p\mathbb{Z}$ has a unique cube root. So, each choice of $y \in \mathbb{Z}/p\mathbb{Z}$ yields a unique x with $y^2 - B = x^3$. Therefore, counting the point at infinity, there are indeed $p + 1$ elements in $E_p(\mathbb{Z}/p)$.

As in the previous Proposition, we see that $6 | \#E(\mathbb{Q})_{\text{tor}}$ by using Dirichlet's theorem (to see that 4 does not divide the order, consider $p \equiv 5 \pmod{12}$, to see that 9 does not divide the order, consider $p \equiv 2 \pmod 9$, and to see that $q > 3$ does not divide the order, consider $p \equiv 2 \pmod{3q}$).

A point $P = (x, y) \neq \mathcal{O}$ has order 3 if and only if $2P = -P$, which holds if and only if $x(2P) = x(P)$ (because $2P = P$ implies $P = \mathcal{O}$, which is assumed not to be the case). Using the formula for $x(2P)$, we conclude that $2P = -P$ is equivalent to

$$\frac{x^4 - 8Bx}{4(x^3 + B)} = x \iff x^4 = -4Bx.$$

So, $x = 0$ gives a point of order 3 if and only if B is a square ($x = 0$ yields $y^2 = B$). The other possible solution is x such that $x^3 = -4B$; then $y^2 = x^3 + B = -3B$. Recall that B is not divisible by sixth powers of primes,

hence the only possible primes that divide B are 2 and 3, and $B < 0$. We write $B = -2^a 3^b$ and see that $B = -2^4 3^3$. Thus, $E(\mathbb{Q})$ has an element of order 3 if and only if B is a square or $B = -2^4 3^3$. We know that $E(\mathbb{Q})$ has an element of order 2 if and only if $x^3 + B$ has a rational solution, which is the case if and if B is a cube. So, when $B = 1$, the torsion group has elements of order 2 and 3, and is, therefore, isomorphic to $\mathbb{Z}/6$. If $B \neq 1$ is a square, then B is not a cube, since it is not divisible by sixth powers of primes, so the torsion group has an element of order 3, but not of order 2. This is also the case when $B = -2^4 3^3$, so in these two cases, $E(\mathbb{Q})_{\text{tor}} \simeq \mathbb{Z}/3$. If $B \neq 1$ is a cube, we have an element of order 2 but not of order 3, so the torsion group is isomorphic to $\mathbb{Z}/2$, which completes the proof. □

5 Application to congruent numbers.

A square–free integer $n \geq 1$ is called a congruent number if one of the following three equivalent conditions is satisfied:

1. n is the area of a Pythagorean triangle with rational sides;
2. There is a rational number x such that $x - n, x, x + n$ are all perfect squares.
3. There is a nontrivial rational point on the elliptic curve
$$y^2 = x^3 - n^2 x.$$

It is easy to see that the first two conditions are equivalent because if n satisfies one of them, we can explicitly construct either the Pythagorean triple of the rational number x. Also, if $x-n, x, x+n$ are all perfect squares, then their product is a square, hence the there is a nontrivial rational point on the elliptic curve. The last implication is nontrivial. If (x_0, y_0) is a nontrivial rational point on the elliptic curve, then $y_0 \neq 0$, so $2(x_0, y_0) = (x_1, y_1)$ and Theorem 1 implies that $y_1 - n, y_1, y_1 + n$ are all perfect squares, since the roots of the cubic are precisely $0, \pm n$.

Theorem 12. *A square–free positive integer n is congruent if and only if the rank r of the elliptic curve*
$$E : y^2 = x^3 - n^2 x$$
satisfies $r \geq 1$.

Proof. Assume first $r = 0$. Then $E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tor}} \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/2$ (by Proposition 10), so there are no nontrivial rational points on E, hence n is not congruent. The converse is obvious. □

For example, $n = 1$ is not congruent because the cubic equation defining the elliptic curve $y^2 = x^3 - x$ has as roots $0, \pm 1$, and thus 2 is the only bad prime, which is fairly bad. Therefore, $n_1 = 1, n_2 = 0$, and so $r \leq n_1 + 2n_2 - 1 = 0$, proving that $r = 0$, hence 1 is not congruent.

References

[1] Cremona, J.,

`http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/mwrank.info`

[2] Doud, D. "A procedure to calculate torsion of elliptic curves over $\mathbb{Q}$," *Manuscripta Mathematica.* **95.** 1998, 463–369.

[3] Kato, K., *Number Theory 1: Fermat's Dream,* 2000. American Mathematical Society.

[4] Knapp, A. *Elliptic Curves,* 1992. Princeton University Press.

[5] Li, D., "Proving Mordell-Weil: A Descent in Three Parts" (Senior Thesis, 2005).

[6] Silverman, J., Tate, J. *Rational Points on Elliptic Curves,* 1992. Springer–Verlag. New York Inc.

[7] Stein, W., "Lecture 27: Torsion poins on elliptic curves and Mazur's big theorem," Harvard University, Math 124, Fall 2001.